[033] Abstract

A simplified signing algorithm of the RSA formula is as follows:

Sign

$$\mathbf{Sx} = \mathbf{Mx}\ \{\mathbf{Cx}\} = \mathbf{Cx}^{\mathbf{Mx}} \pmod{\mathbf{no}}$$

Verify

$$\begin{aligned} &\mathbf{Eo}\ \{\mathbf{Sx}\} \\ &= \mathbf{Sx}^{\mathbf{eo}} \pmod{\mathbf{no}} \\ &= \mathbf{Cx}^{\mathbf{Mx*eo}} \pmod{\mathbf{no}} \\ &= \mathbf{Nx}^{\mathbf{do*Mx*eo}} \pmod{\mathbf{no}} \\ &= \mathbf{Nx}^{\mathbf{Mx}} \pmod{\mathbf{no}} \end{aligned}$$

Since $\mathbf{Nx}^{\mathbf{do*eo}} \pmod{\mathbf{no}} = \mathbf{Nx}$

where

Nx : ID # of Entity **X**, License # issued to Entity **X**
Do : Private Key of System Authority **O**
Eo : Public Key of System Authority **O**
no : Modulus of the key pair **Do**, **Eo**
Cx : Secret Key of **X** where $\mathbf{Cx} = \mathbf{Nx}^{\mathbf{do}} \pmod{\mathbf{no}}$
Mx : Message sent by **X**
Sx : Message signed by **X**